Subject Code : P8ITE12

ELECTIVE COURSE III -6- NETWORK SECURITY

UNIT I

Introduction – Primer on a Networking – Active and Passive Attacks – Layers and Cryptography – authorization – Viruses, worms. The Multi level Model of Security – Cryptography – Breaking an Encryption Scheme – Types of Cryptographic functions – secret key Cryptography – Public key Cryptography – Hash algorithms. Secret key cryptography – Data encryption standard – International Data Encryption Algorithm (IDEA) Modes 4 Operations – Encrypting a Large message – Electronic code book, cipher block chaining, OFB, CFB, CTR – Generating MACs.

UNIT II

Introduction to public key algorithms – Model of arithmetic – Modular addition, Multiplication,
Exponentiation. RSA – RSA Algorithm – RSA Security – Efficiency of RSA – Public Key cryptography Standard (PKCS) - Digital Signature Standard – DSS Algorithm – Working of Verification procedure – Security and DSS – DSS controversy.

UNIT III

Authentication – Overview of authentication systems – password based authentication – Add nets based authentication – cryptographic authentication protocols – who is seeing authenticate – passwords as cryptographic keys – Eaves dropping and server database reading – Trusted intermediaries – Session key establishment. Authentication of people – passwords – online – off line password of using – Eavesdropping – passwords and careless users – Initial Password distribution – Authentication tokens.

UNIT IV

Standards and IP security – Introduction to Kerberos – Tickets and Ticket granting tickets. Configuration - logging into the network – replicated KDCs. Overview of IP security – security associations – security association database - security policy database, AH and ESP – Tunnel Transport mode why protect – IP Header IPV4 and IPV6, NAT, Firewalls, IPV4, IPV6 Authentication Header – ESP.

UNIT V

Network Security Application – Email Security – distribution lists – store and forward – security services for email – establishing keys privacy – authentication of the source – massage Integrity – Non- Repudiation – Proof of submission – Proof of delivery. Message flow confidentially – Anonymity – Names and Addresses. Firewalls – packet filters – application level gateway – encrypted tunnels – comparisons why firewalls don't work – denial of service

attacks. Web security – Introduction –URLs/URIs – HTTP – HTTP digest authentication. Cookies – other web security problems.

TEXT BOOK

1. **Charlie Kaufman, Radia Perlman and Mike Speciner,** "Network Security: Private Communication in a Public Work", Second Edition, Pearson Education/Prentice Hall of India, Delhi, 2002.
2. **MAIWALD, Eric**, Network security – A begineer's guide, Second edition, Tata- McGraw Hill, 2003 (ISBN 0-07-058241-6)

REFERENCES

1. **William Stallings**, "Network Security: Essentials Applications and Standards", Pearson Education, Delhi, 2002.
2. **Hans**, "Information and Communication Security", Springer verlag, 1998.
3 **Derek Atkins**, "Internet Security", Tech media, 1998.